(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 936 812 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.08.1999 Bulletin 1999/33

(51) Int. Cl.[6]: **H04N 5/913**

(21) Application number: **98401513.1**

(22) Date of filing: **18.06.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **13.02.1998 EP 98400344**

(71) Applicant:
CANAL+ Société Anonyme
75711 Paris Cedex 15 (FR)

(72) Inventors:
- **Maillard, Michael**
  28130 Maintenon (FR)
- **Benardeau, Christian**
  77600 Bussy Saint Georges (FR)

(74) Representative:
Cozens, Paul Dennis et al
Mathys & Squire
100 Grays Inn Road
London WC1X 8AL (GB)

(54) Method and apparatus for recording of encrypted digital data

(57) A method of recording transmitted digital data in which transmitted digital information CW 96 is encrypted 97 using a recording encryption key E(NE) 98 and the resulting encrypted ECM message 99 stored on recording support medium. An equivalent of the recording encryption key E(NE) 100 is further encrypted by a recording transport key RT(A) 102 to form an EMM message 103 stored on the support medium together with the encrypted ECM message 99.

Fig.10.

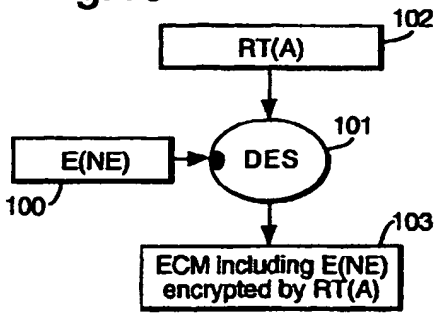
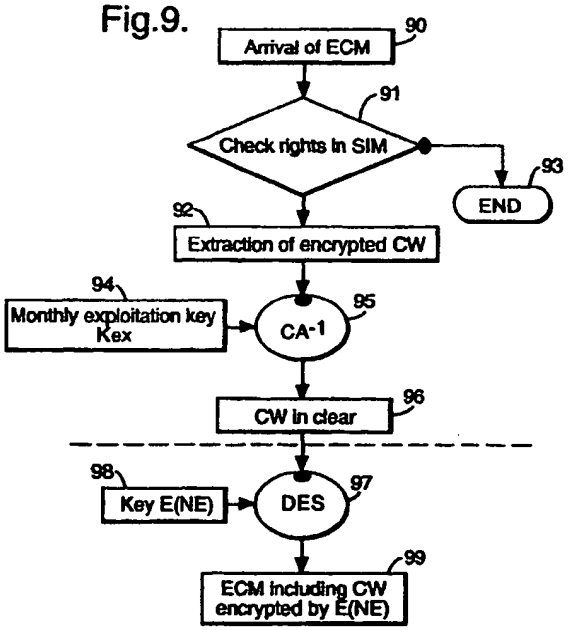


Fig.9.



BEST AVAILABLE COPY

EP 0 936 812 A1

explained in further detail below, the transmitted information may be in some cases processed and/or reencrypted by the decoder before being communicated to the recording means.

[0015] The decoder means may itself be associated with a portable security module used to store transmission access control keys used to decrypt the transmitted encrypted information. In some embodiments, this may be distinct from the portable security module associated with the recording means. However, in the case of an integrated decoder/recorder, for example, the same security module may be used to hold all keys.

[0016] In one embodiment, the recording encryption key and/or recording transport key function in accordance with a first encryption algorithm and the transmission access control keys function in accordance with a second encryption algorithm.

[0017] For example, the recording encryption and transport keys may use the symmetric DES algorithm, whilst the transmission keys function in accordance with a customised algorithm, unique to the broadcast access control system. This enables the system manager to retain control over the algorithm chosen for the transmission keys whilst allowing a generic algorithm to be used for the keys relating to a recording.

[0018] In one embodiment, the recording transport key is generated at a central recording authorisation unit and a copy of this key communicated to the recording means. In the event of loss or destruction of the key support associated with the recording means a backup copy or at least the means to generate the the transport key will at all times be present at the central recording authorisation unit.

[0019] For security reasons, the recording transport key is preferably encrypted by a further encryption key prior to being communicated to the recording means. This further encryption key may be based, for example, on an encryption key common to all recorder security modules diversified by the serial number of the security module, such that only that security module can read the message.

[0020] In the case where the system comprises a receiver/decoder physically separate from the recording means it may be desirable for the recording means to possess the same access rights as the receiver/decoder, for example to permit the receiver/decoder to simply forward the data stream "as is" to the recorder for processing.

[0021] Accordingly, in one embodiment, a central access control system communicates transmission access control keys to a portable security module associated with the recording means. These may comprise, for example, a double of the keys normally held by the portable security module associated with the decoder and which are used to descramble transmissions.

[0022] In this embodiment, the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium.

[0023] In a similar manner as with the communication of the transport key, the central access control system preferably encrypts the broadcast access control keys by a further encryption key prior to their communication to the recording means. This further encryption key may equally comprise an audience key common to all security modules diversified by the serial number of the recording means.

[0024] In order to enable the central access control system to correctly identify the broadcast access keys that need to be forwarded to the recording means, the recording means preferably sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authentified by the recording means using a key unique to the recording means. This may correspond, for example, to the key used to encrypt communications from the central access control system to the recording means.

[0025] In the above realisations of the invention, a number of diverse embodiments have been described, in particular in which a central recording authorisation unit generates and maintains a copy of the recording transport keys and in which a central access control system sends a duplicate set of transmission access control keys to the recording means. Alternative embodiments are possible.

[0026] For example, in one embodiment comprising a decoder means and associated security module and a recording means and associated security module, a copy of the recording transport key is stored in the security module associated with the decoder means. In this way, a backup key for decrypting a recording will always be available even in the event of destruction or loss of the recorder security module.

[0027] The recording transport key may be generated, for example, by the recording means security module and communicated to the decoder means security module or vice versa. For security reasons, the recording transport key is preferably encrypted before communication to the decoder security module and decrypted by a key unique to the security module receiving the recording transport key.

[0028] This unique key and its equivalent may be embedded in the respective security modules at the moment of their creation. However, alternatively, the decoder security module and recording security module carry out a mutual authorisation process, the unique decryption key being passed to the other security module from the encrypting security module depending on the results of the mutual authorisation.

[0029] In one embodiment, the mutual authorisation step is carried out using, inter alia, an audience key known to both security modules diversified by the serial number of each module.

[0030] In a further development of this double security

recording support according to this second embodiment; and

Figure 20 shows communication between a decoder card and a recorder card.

[0038] An overview of a digital television broadcast and reception system 1 is shown in Figure 1. The invention includes a mostly conventional digital television system 2 which uses the MPEG-2 compression system to transmit compressed digital signals. In more detail, MPEG-2 compressor 3 in a broadcast centre receives a digital signal stream (for example a stream of audio or video signals). The compressor 3 is connected to a multiplexer and scrambler 4 by linkage 5. The multiplexer 4 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 6 of the broadcast centre via linkage 7, which can of course take a wide variety of forms including telecom links.

[0039] The transmitter 6 transmits electromagnetic signals via uplink 8 towards a satellite transponder 9, where they are electronically processed and broadcast via a notional downlink 10 to earth receiver 11, conventionally in the form of a dish owned or rented by the end user. The signals received by receiver 11 are transmitted to an integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 decodes the compressed MPEG-2 signal into a television signal for the television set 13.

[0040] A conditional access system 20 is connected to the multiplexer 4 and the receiver/decoder 12, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smartcard, capable of decrypting messages relating to commercial offers (that is, one or several television programmes sold by the broadcast supplier), can be inserted into the receiver/decoder 12. Using the decoder 12 and smartcard, the end user may purchase events in either a subscription mode or a pay-per-view mode.

[0041] An interactive system 17, also connected to the multiplexer 4 and the receiver/decoder 12 and again located partly in the broadcast centre and partly in the decoder, may be provided to enable the end user to interact with various applications via a modemmed back channel 16.

[0042] The conditional access system 20 will now be described in more detail. With reference to Figure 2, in overview the conditional access system 20 includes a Subscriber Authorization System (SAS) 21. The SAS 21 is connected to one or more Subscriber Management Systems (SMS) 22, one SMS for each broadcast supplier, by a respective TCP-IP linkage 23 (although other types of linkage could alternatively be used). Alternatively, one SMS could be shared between two broadcast suppliers, or one supplier could use two SMSs, and soon.

[0043] First encrypting units in the form of ciphering units 24 utilising "mother' smartcards 25 are connected to the SAS by linkage 26. Second encrypting units again in the form of ciphering units 27 utilising mother smartcards 28 are connected to the multiplexer 4 by linkage 29. The receiver/decoder 12 receives a portable security module, for example in the form of "daughter" smartcard 30. It is connected directly to the SAS 21 by Communications Servers 31 via the modemmed back channel 16. The SAS sends, amongst other things, subscription rights to the daughter smartcard on request.

[0044] The smartcards contain the secrets of one or more commercial operators. The "mother" smartcard encrypts different kinds of messages and the "daughter" smartcards decrypt the messages, if they have the rights to do so.

[0045] The first and second ciphering units 24 and 27 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one smartcard 25 and 28 respectively, for each electronic card, one card 28 for encrypting the ECMs and one card 25 for encrypting the EMMs.

[0046] The operation of the conditional access system 20 of the digital television system will now be described in more detail with reference to the various components of the television system 2 and the conditional access system 20.

Multiplexer and Scrambler

[0047] With reference to Figures 1 and 2, in the broadcast centre, the digital audio or video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 3. This compressed signal is then transmitted to the multiplexer and scrambler 4 via the linkage 5 in order to be multiplexed with other data, such as other compressed data.

[0048] The scrambler generates a control word used in the scrambling process and included in the MPEG-2 stream in the multiplexer. The control word is generated internally and enables the end user's integrated receiver/decoder 12 to descramble the programme.

[0049] Access criteria, indicating how the programme is commercialised, are also added to the MPEG-2 stream. The programme may be commercialised in either one of a number of "subscription" modes and/or one of a number of "Pay Per View" (PPV) modes or events. In the subscription mode, the end user subscribes to one or more commercial offers, or "bouquets", thus getting the rights to watch every channel inside those bouquets. In the preferred embodiment, up to 960 commercial offers may be selected from a bouquet of channels.

[0050] In the Pay Per View mode, the end user is provided with the capability to purchase events as he wishes. This can be achieved by either pre-booking the

nal for onward transmission to television set 13.

Subscriber Management System (SMS)

[0062] A Subscriber Management System (SMS) 22 includes a database 32 which manages, amongst others, all of the end user files, commercial offers, subscriptions, PPV details, and data regarding end user consumption and authorization. The SMS may be physically remote from the SAS.

[0063] Each SMS 22 transmits messages to the SAS 21 via respective linkage 23 which imply modifications to or creations of Entitlement Management Messages (EMMs) to be transmitted to end users.

[0064] The SMS 22 also transmits messages to the SAS 21 which imply no modifications or creations of EMMs but imply only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).

[0065] The SAS 21 sends messages (typically requesting information such as call-back information or billing information) to the SMS 22, so that it will be apparent that communication between the two is two-way.

Subscriber Authorization System (SAS)

[0066] The messages generated by the SMS 22 are passed via linkage 23 to the Subscriber Authorization System (SAS) 21, which in turn generates messages acknowledging receipt of the messages generated by the SMS 21 and passes these acknowledgements to the SMS 22.

[0067] In overview the SAS comprises a Subscription Chain area to give rights for subscription mode and to renew the rights automatically each month, a Pay Per View Chain area to give rights for PPV events, and an EMM Injector for passing EMMs created by the Subscription and PPV chain areas to the multiplexer and scrambler 4, and hence to feed the MPEG stream with EMMs. If other rights are to be granted, such as Pay Per File (PPF) rights in the case of downloading computer software to a user's Personal Computer, other similar areas are also provided.

[0068] One function of the SAS 21 is to manage the access rights to television programmes, available as commercial offers in subscription mode or sold as PPV events according to different modes of commercialisation (pre-book mode, impulse mode). The SAS 21, according to those rights and to information received from the SMS 22, generates EMMs for the subscriber.

[0069] The EMMs are passed to the Ciphering Unit (CU) 24 for ciphering with respect to the management and exploitation keys. The CU completes the signature on the EMM and passes the EMM back to a Message Generator (MG) in the SAS 21, where a header is added. The EMMs are passed to a Message Emitter (ME) as complete EMMs. The Message Generator determines the broadcast start and stop time and the rate of emission of the EMMs, and passes these as appropriate directions along with the EMMs to the Message Emitter. The MG only generates a given EMM once; it is the ME which performs cyclic transmission of the EMMs.

[0070] On generation of an EMM, the MG assigns a unique identifier to the EMM. When the MG passes the EMM to the ME, it also passes the EMM ID. This enables identification of a particular EMM at both the MG and the ME.

[0071] In systems such as simulcrypt which are adapted to handle multiple conditional access systems e.g. associated with multiple operators, EMM streams associated with each conditional access system are generated separately and multiplexed together by the multiplexer 4 prior to transmission.

Encryption Levels of the System

[0072] Referring now to Figure 3, a simplified outline of the encryption levels in the broadcast system will now be described. The stages of encryption associated with the broadcast of the digital data are shown at 41, the transmission channel (eg a satellite link as described above) at 42 and the stages of decryption at the receiver at 43.

[0073] The digital data N is scrambled by a control word CW before being transmitted to a multiplexer Mp for subsequent transmission. As will be seen from the lower part of Figure 3, the transmitted data includes an ECM comprising, inter alia, the control word CW as encrypted by an encrypter Ch1 controlled by a first encryption key Kex. At the receiver/decoder, the signal passes by a demultiplexer DMp and descrambler D before being passed to a television 2022 for viewing. A decryption unit DCh1 also possessing the key Kex decrypts the ECM in the demultiplexed signal to obtain the control word CW subsequently used to descramble the signal.

[0074] For security reasons, the control word CW embedded in the encrypted ECM changes on average every 10 seconds or so. In contrast, the first encryption key Kex used by the receiver to decode the ECM is changed every month or so by means of an operator EMM. The encryption key Kex is encrypted by a second unit ChP using a personalised group key K1(GN). If the subscriber is one of those chosen to receive an updated key Kex, a decryption unit DChP in the decoder will decrypt the message using its group key K1(GN) to obtain that month's key Kex.

[0075] The decryption units DChp and DCh1 and the associated keys are held on a smart card provided to the subscriber and inserted in a smart card reader in the decoder. The keys may be generated, for example, according to any generally used symmetric key algorithm or in accordance with a customised symmetric key

are more usually created by means of a special transmitted EMM message at the start up of a decoder.

[0088] As mentioned above, the operator keys may typically include a K0' diversified by a number NS unique to that card, a group key K1' diversified by a group number GN and an audience key K2' diversified by a constant Z and common to all subscriber card addressed by that operator.

[0089] Finally, the smart card includes the value of the unique number NS of that card, implanted at the moment of personalisation and held in the zone 57 of the smart card memory.

[0090] As is shown, the SIM card 52 associated with the digital recorder includes two sections 58, 59 associated with keys and operations carried out using the CA and DES algorithms, respectively. The section 59 associated with operations using the CA algorithm includes a first system manager zone 60 and an operator zone 61. The keys in the system manager zone are implanted in the card at the moment of personalisation by the conditional access system manager and include a key K0 diversified by the serial number NSIM of the SIM card as well as a communications transport key T also diversified by the serial number NSIM of the card. Both keys are unique to the SIM card in question.

[0091] The SIM card further includes an operator zone 61 adapted to store keys associated with one or more operators. In the present Figure 5, the SIM card is shown as it is at the moment of its creation and personalisation by the conditional access system manager and before insertion in a recorder. For this reason, both the operator zone 61 and the DES zone 58 are shown as blank, i.e. without any stored keys.

[0092] Finally, the SIM card includes a zone 63 adapted to hold the unique SIM card serial number NSIM.

[0093] As mentioned above, in this embodiment, the recorder SIM card 52 is adapted to handle the real time decryption and descrambling of broadcast data autonomously and independent of the smart card 30 associated with the decoder. In order to carry out these operations, it is necessary for the recorder SIM card 52 to possess a double of the keys usually held in the system manager and operator zones 55, 56 of the decoder smart card (see Figure 5). As will be described, once the necessary keys are installed in the recorder SIM card 52, the decoder 12 will thereafter pass the broadcast transmission stream "as is" to the digital recorder 50 and card 52.

[0094] In this embodiment, the generation of duplicate broadcast related keys is managed by the central conditional access system 21, the digital recorder 50 acting to transmit a request to the appropriate server, e.g. via the modem link provided by the decoder 12. Alternatively, it may be envisaged that the recorder itself will be equipped with a modem to carry out this request. In this embodiment, the central conditional access system serves to regulate both transmission access control keys and, as will be described recording access control keys

[0095] In order to enable the central conditional access system server to generate a double of the keys associated with the decoder smart card it is necessary that the request message from the recorder SIM card includes an identification of the identity of the decoder smart card (e.g. the smart card serial number NS) as well as providing secured confirmation of its own identity.

[0096] As a first step therefore, the decoder smart card 30 communicates its serial number NS and a list of operators Op1, Op2 etc. to the SIM card 52. For reasons of security, this communication may itself be encrypted by a simple transport encryption algorithm applied to all communications between the decoder 12 and recorder 50. To avoid unnecessary complexity in the Figures, the keys associated with this encryption are not shown. The decider card serial number NS is then stored in the system manager zone of the SIM card.

[0097] The recorder SIM card 52 then sets up a communication with the conditional access system 21 and requests the unique number NMERE of the conditional access system 21 at the conditional access server (see Figure 2). Using the information thus obtained, the recorder SIM card 52 generates a message using the CA algorithm, as shown in Fig. 6.

[0098] In the convention adopted in the accompanying drawings, the symmetric algorithm to be used in a given cryptographic step (CA or DES) is identified within an oval. The data to be encrypted and/or the data serving as a diversifier is identified as arriving via a blacked out input to the oval. See the encryption of the smart card number and operator list at 70 in Figure 6. Decryption steps are distinguished using an inverse power sign, for example CA^{-1} or DES^{-1}.

[0099] As a first step in Figure 6, the smart card number NS and operator list are encrypted by the key K0 (NSIM) as shown at 70 to generate a message 71 comprising the SIM card serial number NSIM and the encrypted data. At a second step 72, the encrypted data is again re-encrypted by the key T (NSIM, NMERE), created by diversifying the key T (NSIM) by a unique value NMERE associated with the conditional access system. As will be understood, the steps 70, 71 may be carried out in the inverse order. The message 73 and signature thus formed are then sent to the conditional access server 21, ciphering unit 24 and mother card 25.

[0100] The conditional access system 21 decrypts the message as shown in Figure 7. The system possesses the original key K0 shown at 76. Diversifying the key K0 with the NSIM value contained in the message, as shown at 77, generates the key K0 (NSIM). The key K0 (NSIM) is first used to validate the signature at 78. In the event that the signature is not valid, the analysis of the message ends, as shown at 81.

[0101] In addition to the key K0, the system also possesses the transport key T or at least the key T

that the recorder SIM card contains a duplicate of the necessary operator keys to independently decrypt and descramble a real time transmission. The second embodiment, described below in Figures 12 to 19 does not suffer from these constraints, but describes a realisation in which the decoder smart card plays a more important role.

Second Embodiment

[0114] Referring to Figure 12, the structure of the conditional access zones in the decoder smart card 30 and recorder SIM card 52 in such a system are shown. As before, both cards include zones reserved for operations using the CA algorithm and storage of key data, in particular system manager zones 55, 60 and operator zones 56, 61.

[0115] In the present embodiment, the system manager zone 55 of the decoder card 30 includes, in addition to the key K0 (NS), an audience key K1 (C) common to all cards personalised and managed by the system manager and formed by the diversification of a CA key by a constant value C. This key K1 (C) is also present in the system management zone 60 of the recorder card 52.

[0116] The other significant change in comparison with the zone structure of the previous embodiment is that the smart card 30 is additionally provided with the DES algorithm and includes a DES operating zone 120.

[0117] In order to enable the decoder smart card and recorder SIM card to work together and, in particular, to enable the eventual generation of a recording transport key TR, it is necessary for a mutual authentification of both cards to be carried out.

[0118] As shown in Figure 13, as a first step 121 the recorder SIM card 52 requests a random number from the decoder smart card 30 which returns the number A1 at 122. This number is then used to diversify the audience key K1 (C) at step 123 to generate the key K1 (C, A1) shown at step 124. The SIM card then generates a second random number A2 shown at 125, which is in turn encrypted by the key K1 (C, A1) at 126. Before communication to the smart card, this message is again encrypted and signed at 128 by a second key K1 (C, NSIM) shown at 127 and formed by diversifying the audience key K1 (C) by the value NSIM. The message 129 thus formed is sent as a request for serial number NS and associated individual key K0(NS) to the decoder smart card 30.

[0119] Referring to Figure 14, on arrival at the decoder smart card 30, the communicated value NSIM is used by the smart card to generate the key K1 (C, NSIM). The value of A2 is then decrypted at 130 using this key and the key K1 (C, A1) obtained by the smart card using the random number A1 that it had previously generated and stored in its memory.

[0120] This random number value A2 obtained at 131 is then used to diversify the audience key K1 (C) to obtain the key K1 (C, A2) shown at 132. The key K1 (C, A2) then encrypts the smart card unique serial number NS and system key K0 (NS) at 133 to create the message 134.

[0121] As before, this message is then re-encrypted at 135 using the key K1 (C, NSIM) shown at 136 and the message returned to the recorder SIM card 52 as shown at 137.

[0122] The recorder SIM card generates the keys K1 (C, A2) and K1 (C, NSIM) shown at 138 by diversifying the key K1 (C) by the NSIM serial number and the previously generated and memorised random number A2. These keys are used to decrypt at 139 the messages so as to obtain the unique serial number NS and unique system manager key K0 (NS) of the smart card, this information thereafter being recorded in the memory of the recorder SIM card at 140.

[0123] Unlike the previous embodiment, in which doubles of all system manager and operator keys were taken to ensure independent operation of the recorder SIM card, the double key K0 (NS) and the smart card serial number NS are used to set up a session key for recording and to enable secure communication between the cards during a recording session, notably to enable secure communication of a recording transport key.

[0124] In this embodiment, the initial decryption of the CW is handled by the smart card using the operator keys and monthly exploitation keys that it possesses. Whilst it is conceivable that the control word CW could be passed directly to the SIM card during the creation of a recording it is desirable for security reasons to use a session key to transport the control word CW for this purpose.

[0125] Figure 15 shows one way of creating such a key. As shown, the recorder SIM card picks a random key K3 shown at 141 and diversifies this key at 142 with the SIM card serial number NSIM shown at 143. The key K3 may be taken from any one of a number of such keys stored for this purpose in the system manager zone. The CA session key K3 (NSIM) thus created at 144 is then encrypted at 145 using the previously obtained smart card system manager key K0 (NS) shown at 146. The message 147 thus generated is thereafter transmitted to the decoder smart card 55 which uses its key K0 (NS) to decrypt the message at 148 and store the session key K3 (NSIM) in the memory of the card at step 149.

[0126] Referring to Figure 16, the state of the recorder SIM card prior to a recording operation will now be described. The system manager zone 60 includes the smart card key K0 (NS) and the session key K3 (NSIM) as well as the normally present system keys K0 (NSIM) etc. (not shown). In addition, the card creates a DES recording encryption key from a DES key E shown at 150 by diversifying this key at 151 by a random value NE shown at 152. As before, the resulting recording encryption key E (NE) will be used in the re-encryption

usable to descramble a scrambled data transmission also recorded on the support medium.

3. A method as claimed in claim 1 or 2 in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) are stored on a portable security module (52) associated with the recording means (50).

4. A method as claimed in any preceding claim in which the transmitted information is encrypted prior to transmission and received by a decoder means (12) before being communicated to the recording means (50).

5. A method as claimed in claim 4 in which the decoder (50) is associated with a portable security module (30) used to store transmission access control keys (K0(NS), K0'(Op1,NS) etc.) used to decrypt the transmitted encrypted information.

6. A method as claimed in claim 5 in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) function in accordance with a first encryption algorithm (DES) and the transmission access control keys (K0(NS), K0'(Op1,NS)etc.) function in accordance with a second encryption algorithm (CA).

7. A method as claimed in any preceding claim in which the recording transport key (RT(A)) is generated at a central recording authorisation unit (21,24,25) and a copy of this key communicated to the recording means (50).

8. A method as claimed in claim 7 in which the recording transport key (RT(A)) is preferably encrypted by a further encryption key (K0(NSIM)) prior to being communicated to the recording means (50).

9. A method as claimed in any preceding claim in which a central access control system (21,24,25) communicates transmission access control keys (K0(NS), K0'(Op1,NS) etc.) to the recording means (50).

10. A method as claimed in claim 9 in which the transmission access control keys (K0(NS), K0'(Op1,NS) etc.) are communicated to a portable security module (52) associated with the recording means (50).

11. A method as claimed in claim 9 or 10 in which the recording means (50) directly descrambles transmitted information using the transmission access keys (K0(NS), K0'(Op1,NS) etc.) prior to re-encryption of the information by the recording encryption key (E(NE)) and storage on the support medium.

12. A method as claimed in any of claims 9, 10 or 11 in which the central access control system (21, 24, 25) preferably encrypts the broadcast access control keys (K0(NS), K0'(Op1,NS) etc.) by a further encryption key (K0(NSIM)) prior to their communication to the recording means (50).

13. A method as claimed in any of claims 9 to 12 in which the recording means (50) sends a request to the central access control system including information identifying the broadcast access keys needed (K0(NS), K0'(Op1,NS) etc.), the request being authentified by the recording means (50) using a key (K0(NSIM)) unique to that recording means.

14. A method as claimed in claim 1 using a decoder means (12) and associated security module (30) and a recording means (50) and associated security module (52) and in which a copy of the recording transport key (RT(A)) is stored in the security module (30) associated with the decoder means (12).

15. A method as claimed in claim 14 in which the recording transport key (RT(A)) is generated by the recording security module (52) or decoder security module (30) and communicated to the other security module.

16. A method as claimed in claim 15 in which the recording transport key (RT(A)) is preferably encrypted before communication to the other security module and decrypted by a key unique (K0(NS)) to that other security module.

17. A method as claimed in claim 16 in which the decoder security module (30) and recording security module (52) carry out a mutual authorisation process, the unique decryption key (K0(NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorisation.

18. A method as claimed in claim 17 in which the mutual authorisation step is carried out using, inter alia, an audience key K1(C) known to both security modules (30,52) diversified by the serial number (NS, NSIM) of each module.

19. A method as claimed in any of claims 14 to 18 in which the decoder security module (30) possesses transmission access control keys (K0(NS), K0'(Op1,NS) etc.) to decrypt the transmitted information in an encrypted form and a session key (K3(NSIM)) re-encrypt the information prior to communication to the recording security module (52), the recording security module (52) possessing an

Fig.1.

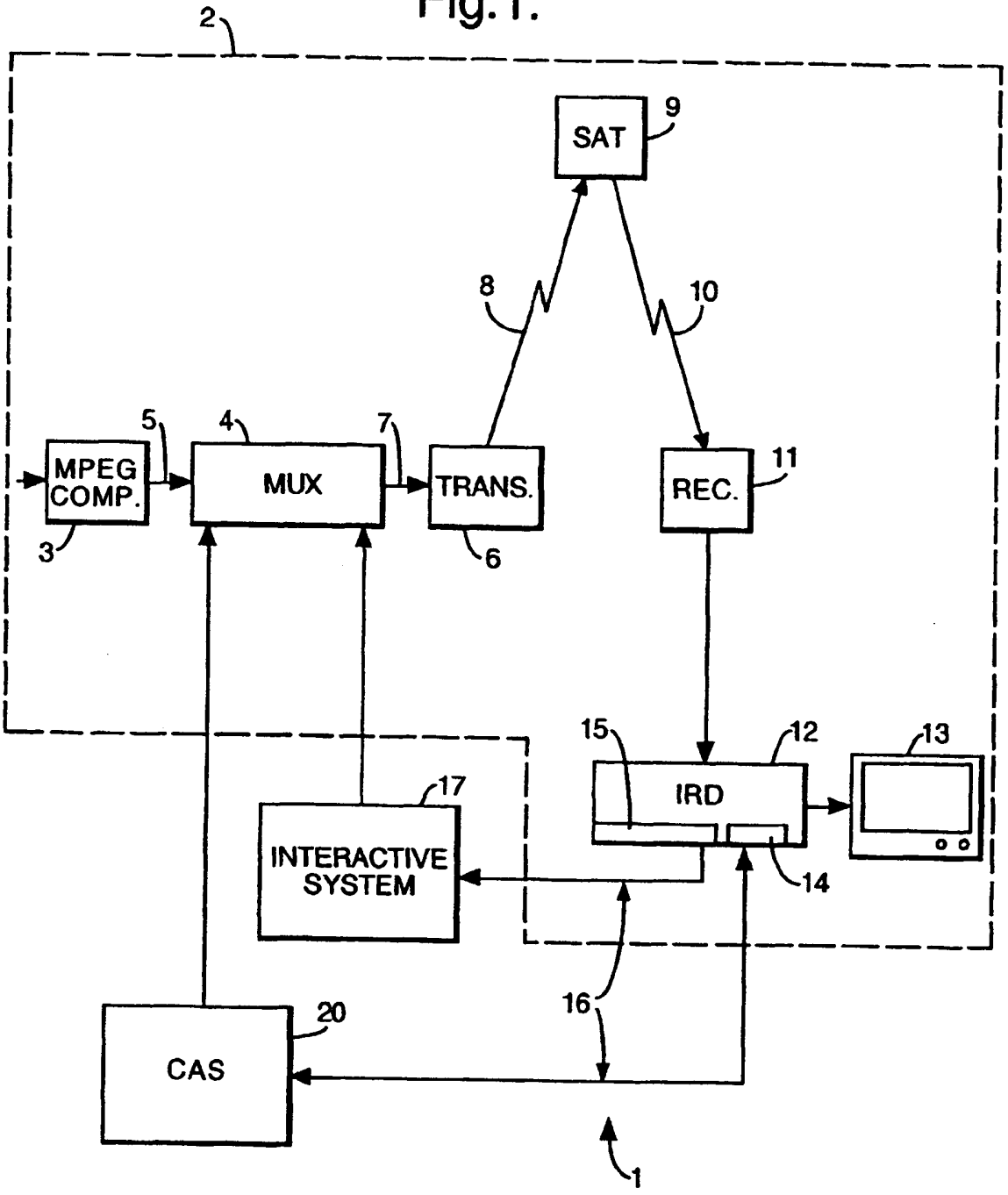
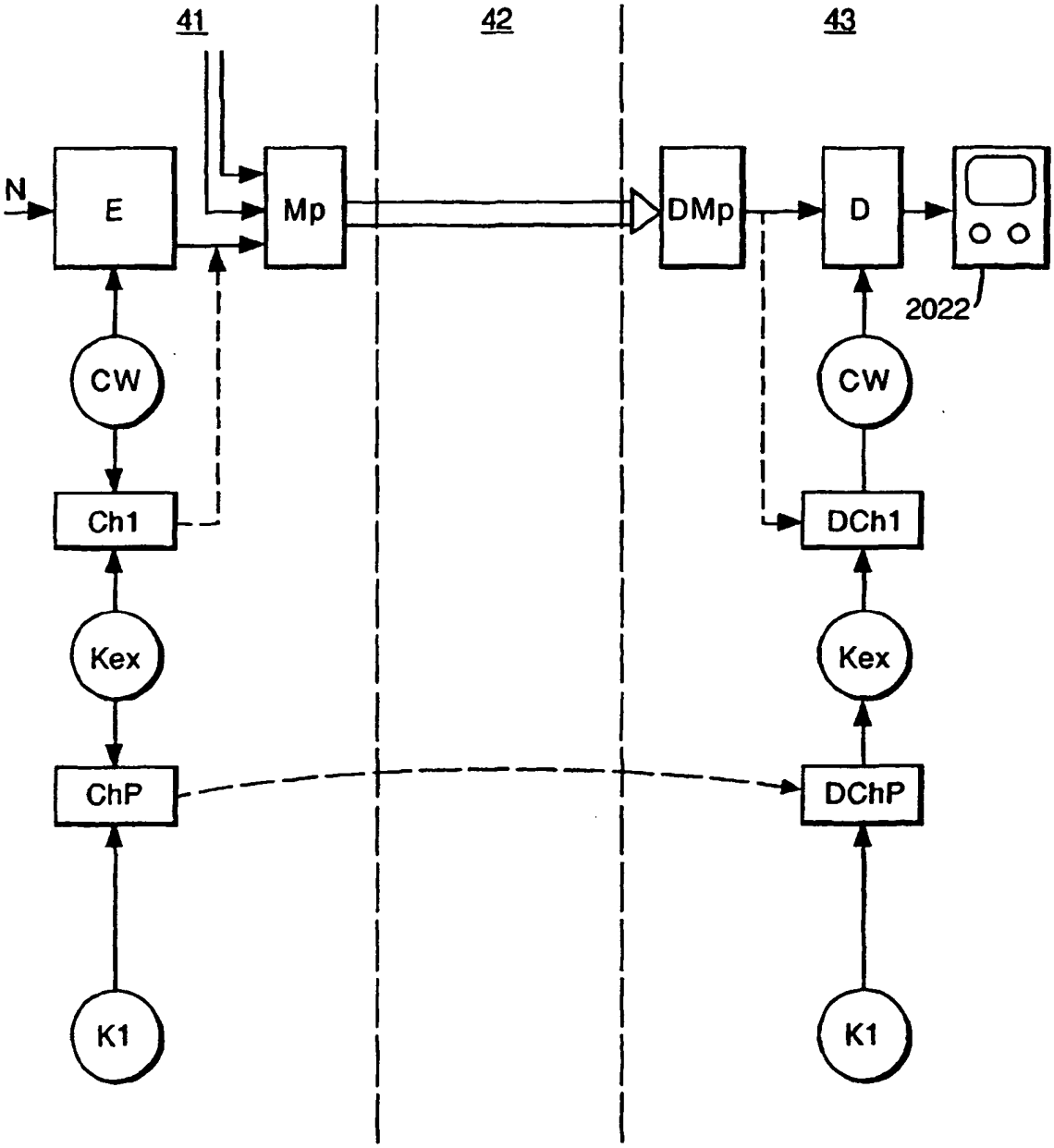

2
SAT
9
8
10
5
4
7
MPEG COMP.
MUX
TRANS.
REC.
11
3
6
15
12
13
IRD
17
INTERACTIVE SYSTEM
14
16
20
CAS
1

Fig.3.


41
42
43
N
E
Mp
DMp
D
2022
CW
CW
Ch1
DCh1
Kex
Kex
ChP
DChP
K1
K1

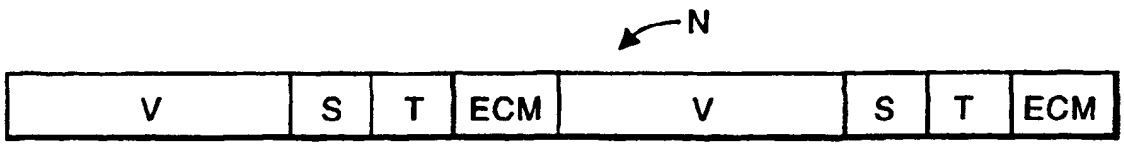

N
V
S
T
ECM
V
S
T
ECM

Fig.5.

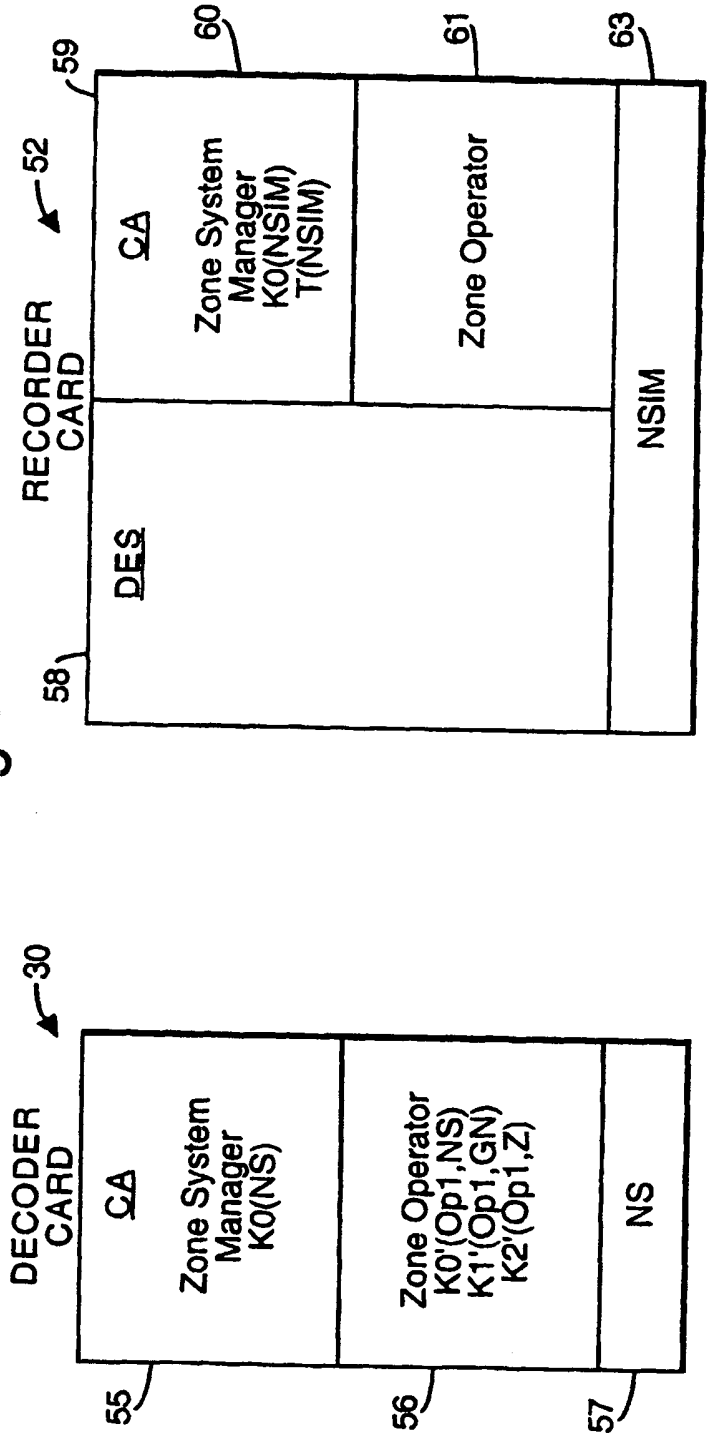

DECODER CARD
30
CA
Zone System Manager K0(NS)
Zone Operator K0'(Op1,NS) K1'(Op1,GN) K2'(Op1,Z)
NS
55
56
57
RECORDER CARD
52
CA
Zone System Manager K0(NSIM) T(NSIM)
Zone Operator
NSIM
DES
58
59
60
61
63

Fig.8.

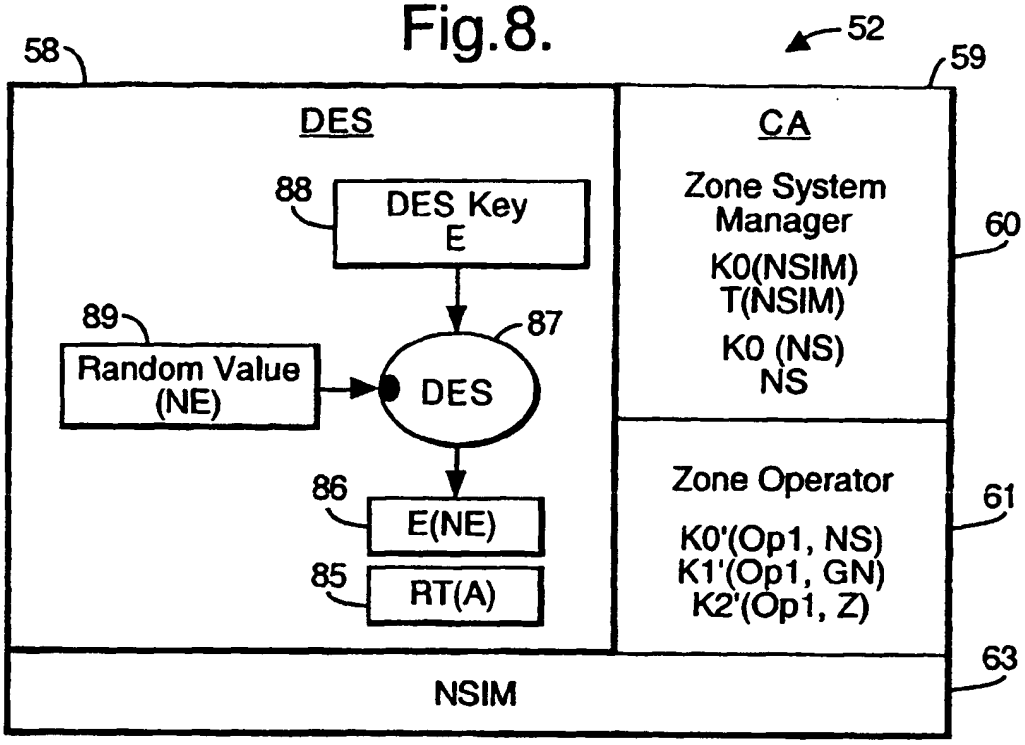

52
58
59
DES
CA
88
DES Key
E
Zone System
Manager
60
K0(NSIM)
T(NSIM)
K0 (NS)
NS
89
87
Random Value
(NE)
DES
86
E(NE)
Zone Operator
61
K0'(Op1, NS)
K1'(Op1, GN)
K2'(Op1, Z)
85
RT(A)
63
NSIM

Fig.11.

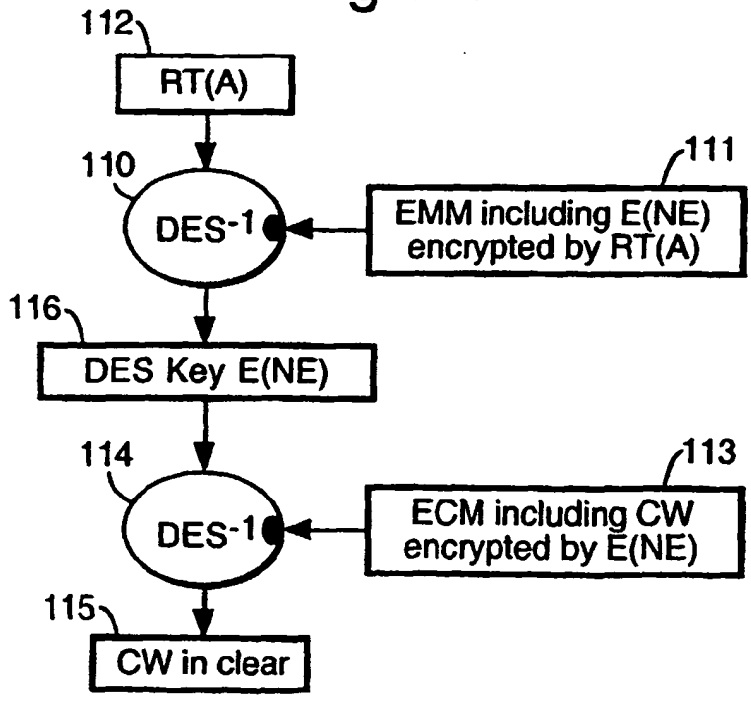

112
RT(A)
110
111
DES-1
EMM including E(NE)
encrypted by RT(A)
116
DES Key E(NE)
114
113
DES-1
ECM including CW
encrypted by E(NE)
115
CW in clear

Fig.12.

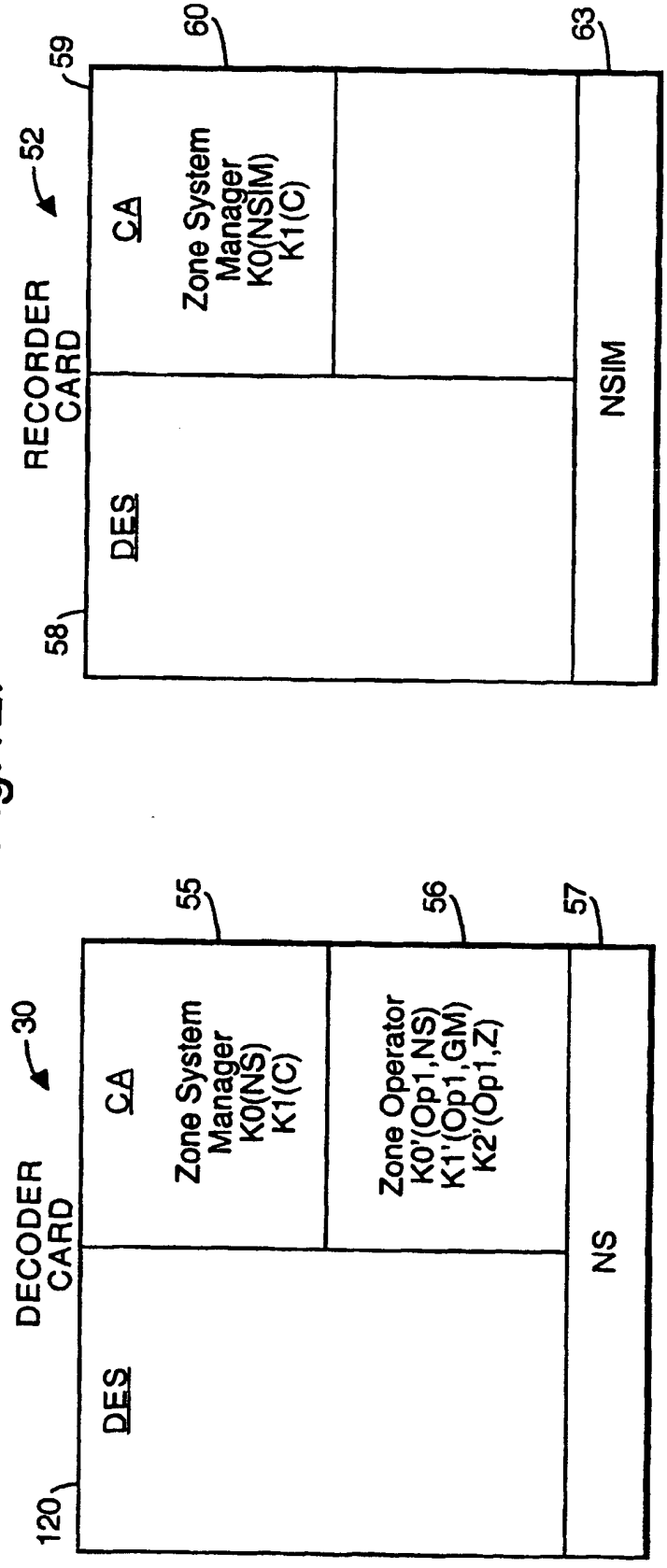

RECORDER CARD
52
59
60
63
CA
Zone System Manager K0(NSIM) K1(C)
DES
NSIM
58
DECODER CARD
30
55
56
57
CA
Zone System Manager K0(NS) K1(C)
Zone Operator K0'(Op1,NS) K1'(Op1,GM) K2'(Op1,Z)
DES
NS
120

Fig.14.

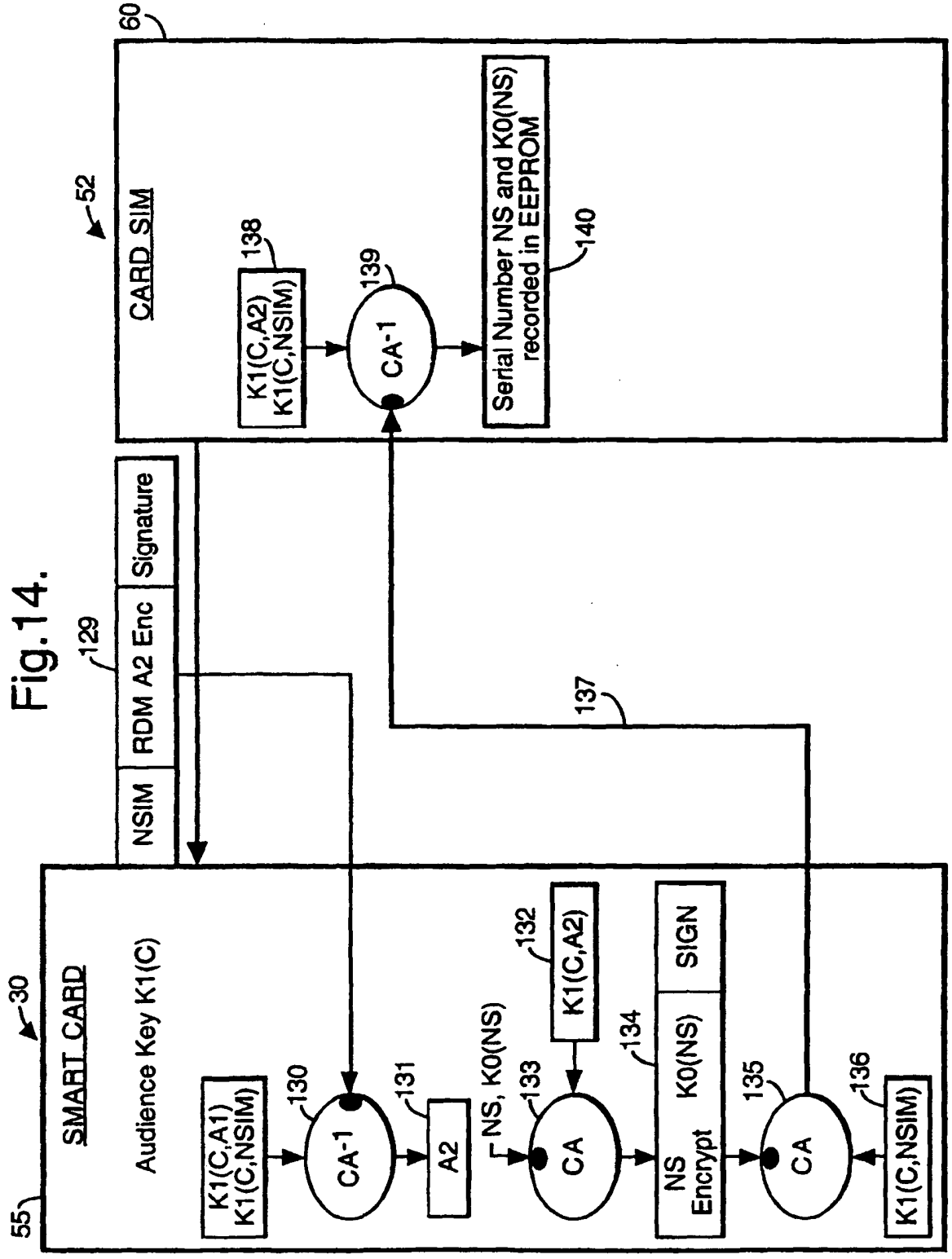
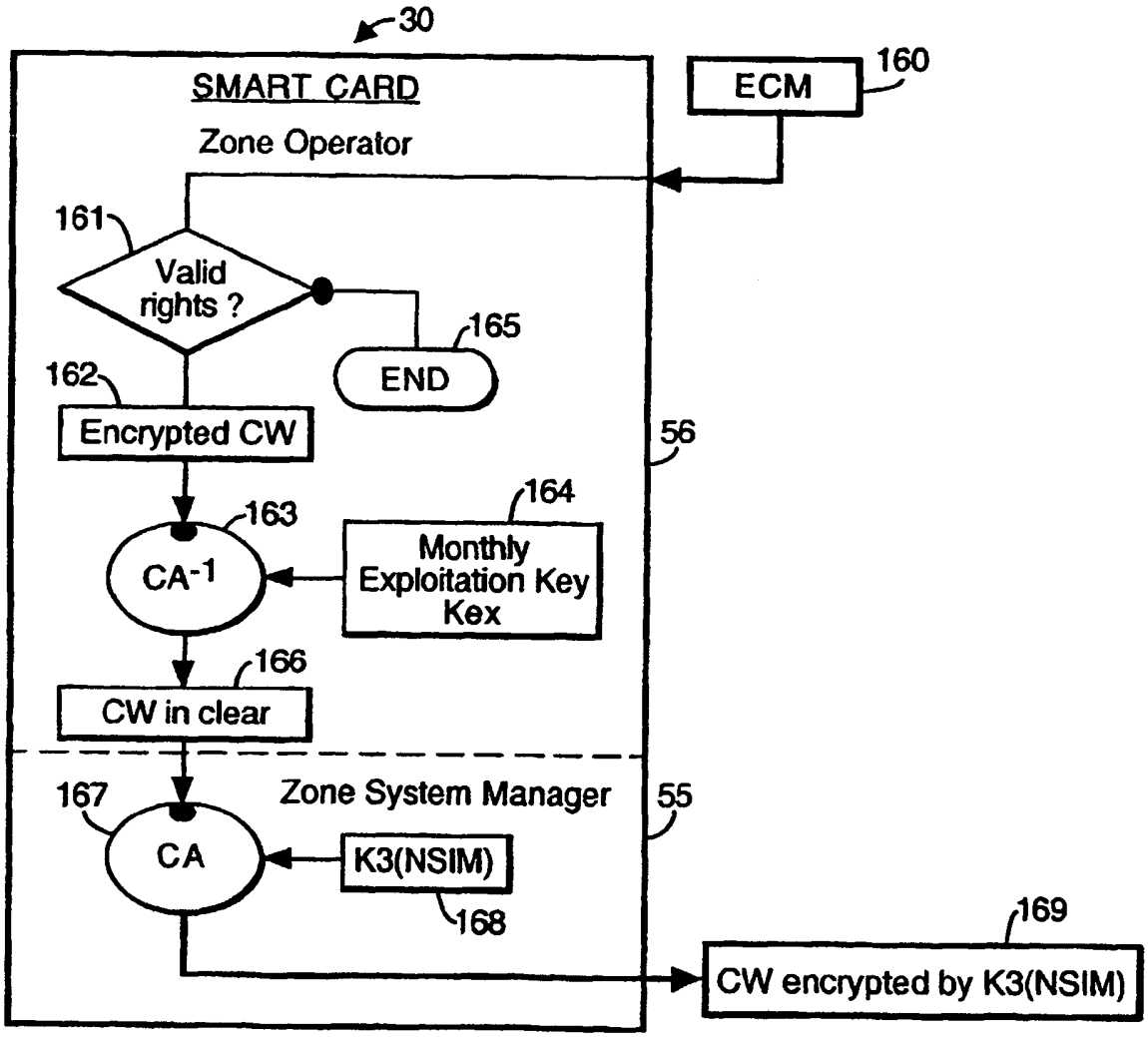

60
52
CARD SIM
138
K1(C,A2)
K1(C,NSIM)
139
CA-1
Serial Number NS and K0(NS) recorded in EEPROM
140
129
NSIM
RDM A2 Enc
Signature
137
30
SMART CARD
Audience Key K1(C)
55
K1(C,A1)
K1(C,NSIM)
130
CA-1
131
A2
NS, K0(NS)
133
CA
132
K1(C,A2)
134
NS Encrypt
K0(NS)
SIGN
135
CA
136
K1(C,NSIM)

Fig.17.


30
SMART CARD
Zone Operator
ECM
160
161
Valid rights ?
165
END
162
Encrypted CW
56
163
164
CA-1
Monthly Exploitation Key Kex
166
CW in clear
167
Zone System Manager
55
CA
K3(NSIM)
168
169
CW encrypted by K3(NSIM)

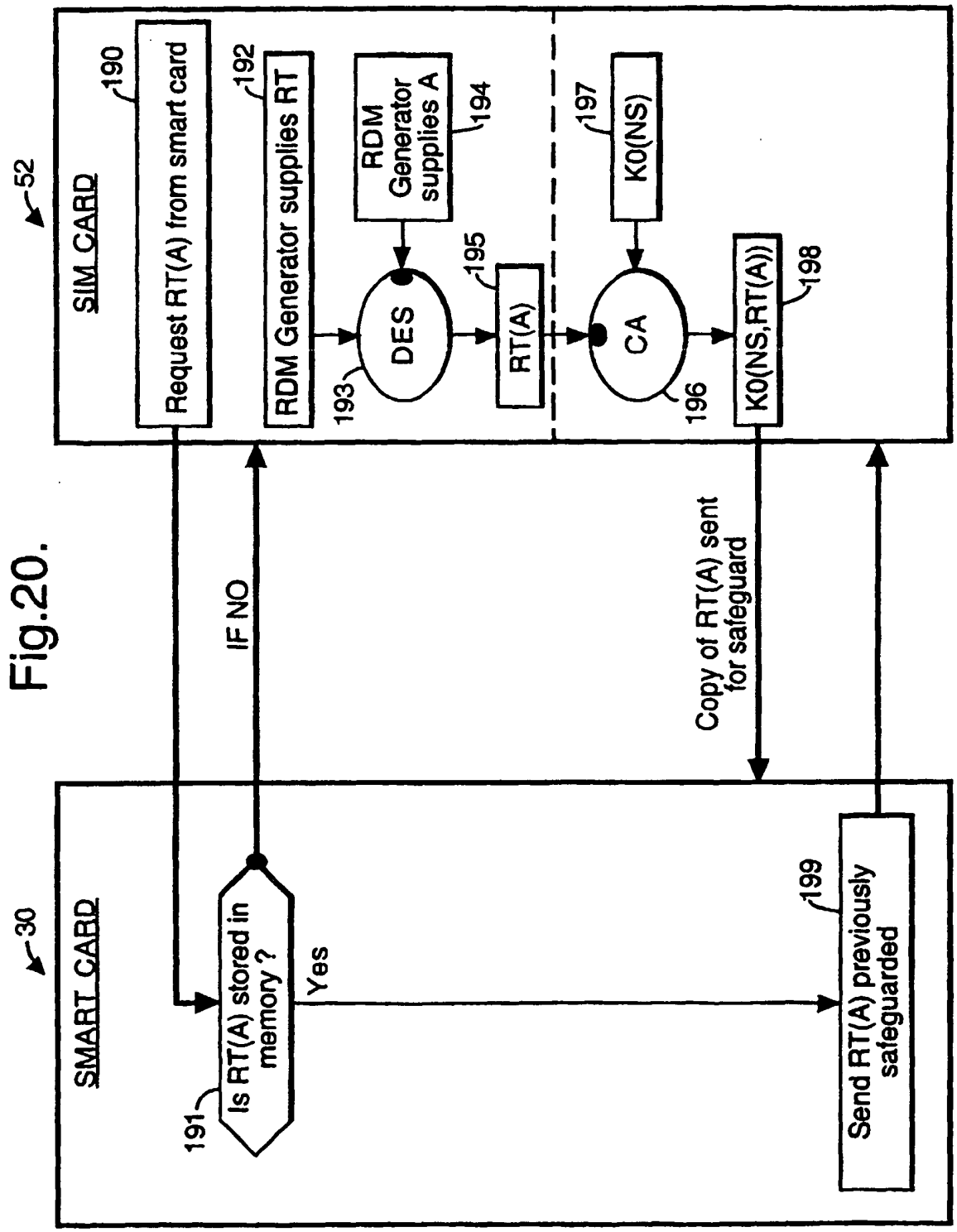

52
SIM CARD
190
Request RT(A) from smart card
192
RDM Generator supplies RT
RDM Generator supplies A
194
197
K0(NS)
193
DES
195
RT(A)
CA
196
K0(NS,RT(A))
198
IF NO
Copy of RT(A) sent for safeguard
30
SMART CARD
Is RT(A) stored in memory ?
191
Yes
199
Send RT(A) previously safeguarded

Fig.20.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 40 1513

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-05-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2732537 A	04-10-1996	NONE	
EP 714204 A	29-05-1996	CN 1137723 A	11-12-1996
		JP 8242438 A	17-09-1996
		US 5757909 A	26-05-1998
EP 763936 A	19-03-1997	CN 1150738 A	28-05-1997
		JP 9093561 A	04-04-1997
		US 5799081 A	25-08-1998